CLAIM REJECTIONS UNDER 35 U.S.C. § 103

OBVIOUSNESS

Examiner submits that claims 46-48, and 50-52 are rejected under 35 U.S.C. 103(a) in view of Sykes, Jr. (US Patent Application Publication 2002/0129108), in view of Byrd in view of Epstein . Applicant respectfully traverses.

U.S.C.§ 103 ANALYSIS

CLAIMS 46-48 AND 50-52 IN VIEW OF EPSTEIN

ANALYSIS OF EPSTEIN SPECIFICATION, AS REFERENCED AND CITED BY THE EXAMINER IN THE OFFICE ACTION

Examiner states that Epstein discloses a method of secure an anonymous electronic messaging via a public network (abstract). Examiner states that Epstein expressly discloses the well know [sic] use of an anonymous remailer which provides: service request comprising that the client's identity be withheld from the intended recipient; the processing unit resending the electronic message to the intended recipient as identified by the client in the registration account; the processing unit notifying the intended recipient that the electronic

message has been sent on behalf of the client by the processing unit (column 1, lines 45-62).[1]

Examiner further states that Epstein shows the method whereby the processing unit clearly identifies a constant and verifiable email address of the processing unit and verifiable contact information of the processing unit , in the email to the intended recipient (i.e. header information which points back to the remailer; column 1, lines 45-62.[2]

Finally, Examiner posits that Epstein shows the method whereby the intended recipient is notified that the intended recipient may choose to post a reply with the processing unit for the originator of the electronic message, (i.e. remailer retains the source address of the message originators for replies to be forwarded, column 1, lines 45-62).[3]

Applicant respectfully traverses and addresses Examiner's objections regarding Epstein in turn. Applicant respectfully submits that the above cited portions of the Epstein specification do not disclose the method of the pending application. Specifically, an analysis of the references to Epstein, as cited by the Examiner, fail to disclose the following novelties of the pending application.

---

[1] Office Action dated September 30th, page 5, paragraph 2 through page 6, paragraph 1.

[2] Office Action dated September 30th, page 9, paragraph 3 through page 10, paragraph 1.

[3] Office Action dated September 30th, page 10, paragraph 2.

1. THE METHOD OF DELIVERY OF THE EMAIL BY THE INDEPENDENT THIRD PARTY TO THE INTENDED RECIPIENT IN THE PENDING APPLICATION IS NOT DISCLOSED BY EPSTEIN

Examiner states in her Office Action[4] that the Epstein abstract discloses the well know [sic] use of an anonymous remailer which provides: service request comprising that the client's identity be withheld from the intended recipient; the processing unit resending the electronic message to the intended recipient as identified by the client in the registration account; the processing unit notifying the intended recipient that the electronic message has been sent on behalf of the client by the processing unit (column 1, lines 45-62).[5]

The Epstein abstract reads as follows:

- A method for secure anonymous querying by a user of an information provider by electronic mail and for obtaining a reply **uses a public key of the provider to form an electronic encrypted query package** containing information including a query, **a generated random number sequence, a hash of the query, a generated public key of the user, and an identification of a public bulletin board.**[6]

The prior art cited by Examiner (column 1, lines 45-62) reads as follows:

- Also, anonymous remailers for electronic mail are known for the purpose of forwarding messages from a message originator to a recipient, with all message header information which could be used to trace the message

---

[4] Application/Control Number 09/982,145, Final Office Action, pp 4-5.

[5] Office Action dated September 30th, page 5, paragraph 2 through page 6, paragraph 1.

[6] US PN 6,023, 510, abstract.

back to its source replaced by information which just points back to the anonymous remailer. It is possible that the message sent to the remailer for forwarding could be an encrypted one, but the destination address would be in the clear because such remailers are generally not **set up to receive and decrypt an encrypted destination address**. Consequently, an eavesdropper monitoring electronic mail messages sent to a remailer could determine both actual source and destination addresses. Also, because the remailer must necessarily retain the source addresses of message originators in order to enable replies to be forwarded, there is the risk that the source addresses could be obtained if the remailer were compromised.

- There is a need to communicate securely and anonymously by transport of electronic messages over a public network such as the Internet to make inquiries and obtain responses thereto, particularly in relation to obtaining information pertaining to health.

Applicant references the Epstein specification to further disclose:
The specific use of a public key as the sole means by which an email is posted a public bulletin board to be retrieved by an intended recipient.

Applicant refers to column 2 line 1, through column 4 line 11 with the pertinent references highlighted.

- It is an object of the present invention to provide a method for queries in the form of electronic messages to be submitted securely and anonymously to an information provider via a public network, such as the Internet, and to provide a method for secure responses by the information provider which are obtainable by the inquiring party.

- Briefly, these and other objects are satisfied by a method, which from the point of view of the user, is for secure anonymous querying of a provider in which:

  a random number sequence, a public key of the user, and a corresponding private key of the user are generated;

  a public key of the provider is used to form an electronic encrypted query package containing information including a query, the generated random number sequence, and the generated public key of the user, the information including an identification of a public bulletin board for posting a message comprising the random number sequence in association with an encrypted response to the query, **and the query package being structured such that the contained information can be obtained by the provider by operations including a decryption with the private key of the provider**; and

  the query package is sent to the provider via a network in a manner that the user is not identifiable to the provider.

- Other aspects of the inventive method from the point of view of the user are that the query package is sent to the provider from a public terminal, and that a hash of the query is generated and is included in the information contained in the query package.

- A further aspect of the present invention is **that a symmetric key of the user is generated and the query package is constructed in a manner that a first part including at least the query is encrypted using the generated symmetric key of the user and**

a second part including at least the generated symmetric key of the user is encrypted using the public key of the provider.

- From the point of view of the information provider, the present invention is directed to a method for secure response by a provider to an anonymous query from a user in which:

an electronic encrypted query package containing information including a query, a random number sequence, **and a public key of the user is received via a network,** the information including an identification of a public bulletin board for posting a message comprising the random number sequence in association with an encrypted response to the query, and the query package being structured such that the contained information can be obtained by the provider by operations including a decryption with the private key of the provider;

the private key of the provider is used to obtain the information in said query package;

the public key of the user is used to form an electronic encrypted response package containing a response to the query, said response package being structured such that the response to the query can be obtained by the user by operations including a decryption with the private key of the user; and

a message comprising the random number sequence in association with the response package is posted to the identified public bulletin board.

- Another aspect of the present invention from the point of view of the server is that a hash of the query is included in the information contained in the query package, and the method further comprises computing a hash of the query, and comparing the computed hash with the hash included in the information.

- Still another aspect of the invention from the point of view of the server is **that the query package is constructed in a manner that a first part including at least the query is encrypted using a symmetric key of the user and a second part including at least the symmetric key of the user is encrypted using the public key of the provider,** and the method further comprises decrypting the second part of the query package using the private key of the provider to obtain at least the symmetric key of the user, and decrypting the first part of the query package using the symmetric key of the user to obtain at least the query.

- The present invention also comprises a stored message on a public bulletin board responsive to an anonymous query, **said message comprising a random number sequence and an associated encrypted electronic response package containing a response to the query**, said response package being structured such that the response to the query can be obtained by the user by operations including a decryption with the private key of the user.

- Another aspect of the inventive stored message is that the response package is constructed in a manner that a first part including at least the response is encrypted using a symmetric key of the provider and a second part **including at least the symmetric key of the provider is encrypted using a public key of a user who made the anonymous query.**

- Other objects, features and advantages of the present invention will become apparent upon perusal of the following detailed description when taken in conjunction with the appended drawing, wherein:

  In a first particular embodiment, the present invention includes a method for secure anonymous querying by **a user of a provider to whom a public key, private key pair is assigned, the public key of the provider being publicly obtainable by the user, the method comprising: formulating by the user of a query to be sent to the provider, generating by the user of a random number sequence, a public key of the user, and a corresponding private key of the user for sole use with said formulated query;** forming an electronic encrypted query package by the user by operations **including encryption with the public key of the provider obtained by the user,** said electronic encrypted query package containing information including the formulated query, the generated random number sequence, the generated public key of the user, and an identification of a public bulletin board for posting a message comprising the random number sequence in association with an encrypted response to the query, and said query package being structured such that the contained information can be obtained by the provider by operations including a decryption with the private key of the provider; and sending by the user of the query package to the provider via a network in a manner that the user is not identifiable to the provider, wherein the generated private key and the generated random number sequence are retained by the user.

- In a first aspect of the first particular embodiment, the method further comprises: receiving by the provider via a network said

query package sent by the user; obtaining by the provider by operations including decryption with the private key of the provider the information in said query package; formulating by the provider of a response to the query; **forming an electronic encrypted response package by the provider by operations include encryption with the public key of the user contained in said query package, said electronic encrypted response package containing the formulated response to the query**, said response package being structured such that the response to the query can be obtained by the user by operations including a decryption with the private key of the user; posting by the provider of a message comprising the random number sequence in association with the response package to the identified public bulletin board; accessing the identified bulletin board by the user in order to download the response package associated with that message posted by the provider including the random number sequence generated by the user; and obtaining by the user by operations including decryption with the private key of the user of the response information in said response package.

Applicant notes the differences between the prior art cited and the pending application regarding the method of delivery of the email. The method of the pending application does not disclose the use of a public key or PKI as a means to posit or post an email for an intended recipient.

///

2. THE METHOD OF IDENTIFYING THE EMAIL ADDRESS SOURCE OF THE REMAILER AND THE EMAIL ADDRESS OF THE INTENDED RECIPIENT IN THE PENDING APPLICATION IS NOT DISCLOSED BY EPSTEIN

Examiner states in her Office Action[7] that the Epstein abstract discloses the well know [sic] use of an anonymous remailer which provides: service request comprising that the client's identity be withheld from the intended recipient; the processing unit resending the electronic message to the intended recipient as identified by the client in the registration account; the processing unit notifying the intended recipient that the electronic message has been sent on behalf of the client by the processing unit (column 1, lines 45-62).[8]

The Epstein abstract reads as follows:

- A method for secure anonymous querying by a user of an information provider by electronic mail and for obtaining a reply uses a public key of the provider to form an electronic encrypted query package containing information including a query, **a generated random number sequence, a hash of the query, a generated public key of the user, and an identification of a public bulletin board.**[9]

The prior art cited by Examiner (column 1, lines 45-62) reads as follows: Also, anonymous remailers for electronic mail are known for the purpose of forwarding messages from a message originator to a recipient, with all message header information which could be used to trace the message back

---

[7] Application/Control Number 09/982,145, Final Office Action, pp 4-5.

[8] Office Action dated September 30th, page 5, paragraph 2 through page 6, paragraph 1.

[9] US PN 6,023, 510, abstract.

to its source replaced by information which just points back to the anonymous remailer. It is possible that the message sent to the remailer for forwarding could be an encrypted one, but the destination address would be in the clear because such remailers are generally not **set up to receive and decrypt an encrypted destination address.** Consequently, an eavesdropper monitoring electronic mail messages sent to a remailer **could determine both actual source and destination addresses**. Also, because the remailer must necessarily retain the source addresses of message originators in order to enable replies to be forwarded, there is the risk that the **source addresses could be obtained if the remailer were compromised.**

Applicant references the Epstein specification to further disclose:
That the source and the identity of the originating email address are not in fact identifiable beyond a numeric code associated with a verifiable website. In fact, Epstein discloses a method whereby an anonymous query is posted on a public board and is retrieved anonymously. In fact, the identities of the originator of the email and the public terminal that transmits it, are unknown to the intended recipient beyond a number. Moreover, the method disclosed by Epstein does not involve the resending of an email, rather a public board whereby the parties may interact anonymously as opposed to identifying the sender and the intended recipient.

Applicant refers to column 2 line 1, through column 4 line 11 with the pertinent references highlighted.

- It is an object of the present invention to provide **a method for queries in the form of electronic messages to be submitted securely and anonymously to an information provider via a public network,** such as the Internet, and to provide a method for secure responses by the information provider which are obtainable by the inquiring party.

- Briefly, these and other objects are satisfied by a method, which from the point of view of the user, is for secure anonymous querying of a provider in which:

  a random number sequence, a public key of the user, and a corresponding private key of the user are generated;

  a public key of the provider is used to form an electronic encrypted query package **containing information including a query, the generated random number sequence, and the generated public key of the user, the information including an identification of a public bulletin board for posting a message comprising the random number sequence in association with an encrypted response to the query**, and the query package being structured such that the contained information can be obtained by the provider by operations including a decryption with the private key of the provider; and

  the query package is sent to the provider via a network in a manner that the user is not identifiable to the provider.

- Other aspects of the inventive method from the point of view of the user are that the query package is sent to the provider from a public terminal, and that a hash of the query is generated and is included in the information contained in the query package.

- A further aspect of the present invention is that a symmetric key of the user is generated and the query package is constructed in a manner that a first part including at least **the query is encrypted using the generated symmetric key of the user and a second**

part including at least the generated symmetric key of the user is encrypted using the public key of the provider.

- From the point of view of the information provider, the present invention is directed to a **method for secure response by a provider to an anonymous query from a user in which**:

an electronic encrypted query package containing information including a query, a random number sequence, and a public key of the user is received via a network, the information including an identification of a public bulletin board for posting a message comprising the random number sequence in association with an encrypted response to the query, and the query package being structured such that the contained information can be obtained by the provider by operations including a decryption with the private key of the provider;

the private key of the provider is used to obtain the information in said query package;

the public key of the user is used to form an electronic encrypted response package containing a response to the query, said response package being structured such that the response to the query can be obtained by the user by operations including a decryption with the private key of the user; and

a message comprising the random number sequence in association with the response package is posted to the identified public bulletin board.

- Another aspect of the present invention from the point of view of the server is that a hash of the query is included in the information contained in the query package, and the method further comprises computing a hash of the query, and comparing the computed hash with the hash included in the information.

- Still another aspect of the invention from the point of view of the server is that the query package is constructed in a manner that a first part including at least the query is encrypted using a symmetric key of the user and a second part including at least the symmetric key of the user is encrypted using the public key of the provider, and the method further comprises decrypting the second part of the query package using the private key of the provider to obtain at least the symmetric key of the user, and decrypting the first part of the query package using the symmetric key of the user to obtain at least the query.

- The present invention also comprises a stored message on a public bulletin board **responsive to an anonymous query**, **said message comprising a random number sequence and an associated encrypted electronic response package containing a response to the query**, said response package being structured such that the response to the query can be obtained by the user by operations including a decryption with the private key of the user.

- Another aspect of the inventive stored message is that the response package is constructed in a manner that a first part including at least the response is encrypted using a symmetric key of the provider and a second part including at least the symmetric key of the provider is encrypted **using a public key of a user who made the anonymous query.**

- Other objects, features and advantages of the present invention will become apparent upon perusal of the following detailed description when taken in conjunction with the appended drawing, wherein:

In a first particular embodiment, the present invention includes a method for secure anonymous querying by a user of a provider to whom a public key, private key pair is assigned, the public key of the provider being publicly obtainable by the user, the method comprising: formulating by the user of a query to be sent to the provider, generating by the user of a random number sequence, a public key of the user, and a corresponding private key of the user for sole use with said formulated query; forming an electronic encrypted query package by the user by operations **including encryption with the public key of the provider obtained by the user, said electronic encrypted query package containing information including the formulated query, the generated random number sequence, the generated public key of the user, and an identification of a public bulletin board for posting a message comprising the random number sequence in association with an encrypted response** to the query, and said query package being structured such that the contained information can be obtained by the provider by operations including a decryption with the private key of the provider; **and sending by the user of the query package to the provider via a network in a manner that the user is not identifiable to the provider, wherein the generated private key and the generated random number sequence are retained by the user.**

- In a first aspect of the first particular embodiment, the method further comprises: receiving by the provider via a network said query package sent by the user; obtaining by the provider by operations including decryption with the private key of the provider the information in said query package; formulating by the provider of a response to the query; **forming an electronic encrypted response package by the provider by operations include encryption with the public key of the user contained in said query package, said electronic encrypted response package containing the formulated response to the query**, said response package being structured such that the response to the query can be obtained by the user by operations including a decryption with the private key of the user; **posting by the provider of a message comprising the random number sequence in association with the response package to the identified public bulletin board**; accessing the identified bulletin board by the user in order to **download the response package associated with that message posted by the provider including the random number sequence generated by the user**; and obtaining by the user by operations including decryption with the private key of the user of the response information in said response package.

Applicant notes the differences between the prior art cited and the pending application regarding the method of delivery of the email. The method of the pending application does not disclose the use of a random sequence number or a public bulletin board whereby all of the parties remain anonymous. **The method of Epstein specifically discloses that the identity of the user is not known to the provider.** The method of the present invention discloses a method whereby the first originator of an email is anonymous to the final recipient but is known to the provider. Moreover, the method of the present

invention discloses a method whereby the remailer is clearly identified and whereby the intended recipient is clearly identified.

3. THE METHOD OF RETRIEVAL OF THE EMAIL BY THE INTENDED RECIPIENT IN THE PENDING APPLICATION IS NOT DISCLOSED BY EPSTEIN

Applicant references the Epstein specification to further disclose:
The specific use of a private key <u>as the sole means by which an email posted on a public bulletin board</u> is used to be retrieved by an intended recipient.

Applicant refers to column 2 line 1, through column 4 line 11 with the pertinent references highlighted.

- It is an object of the present invention to provide a method for queries in the form of electronic messages to be submitted securely and anonymously to an information provider via a public network, such as the Internet, and to provide a method for secure responses by the information provider which are obtainable by the inquiring party.
- Briefly, these and other objects are satisfied by a method, which from the point of view of the user, is for secure anonymous querying of a provider in which:

  a random number sequence, a public key of the user, and a corresponding private key of the user are generated;

  a public key of the provider is used to form an electronic encrypted query package containing information including a query, the generated random number sequence, and the generated public key of the user, **the information including an identification of a**

public bulletin board for posting a message comprising the random number sequence in association with an encrypted response to the query, and the query package being structured such that the contained information can be obtained by the provider by operations including a decryption with the private key of the provider; and

the query package is sent to the provider via a network in a manner that the user is not identifiable to the provider.

- Other aspects of the inventive method from the point of view of the user are that the query package is sent to the provider from a public terminal, and that a hash of the query is generated and is included in the information contained in the query package.

- A further aspect of the present invention is that a symmetric key of the user is generated and the query package is constructed in a manner that a first part including at least the query is encrypted using the generated symmetric key of the user and a second part including at least the generated symmetric key of the user is encrypted using the public key of the provider.

- From the point of view of the information provider, the present invention is directed to a method for secure response by a provider to an anonymous query from a user in which:

an electronic encrypted query package containing information including a query, a random number sequence, and a public key of the user is received via a network, **the information including an identification of a public bulletin board for posting a message comprising the random number sequence in association with**

an encrypted response to the query, and the query package being structured such that the contained information can be obtained by the provider by operations including a decryption with the private key of the provider;

the private key of the provider is used to obtain the information in said query package;

the public key of the user is used to form an electronic encrypted response package containing a response to the query, said **response package being structured such that the response to the query can be obtained by the user by operations including a decryption with the private key of the user; and**

a message comprising the random number sequence in association with the response package is posted to the identified public bulletin board.

- Another aspect of the present invention from the point of view of the server is that a hash of the query is included in the information contained in the query package, and the method further comprises computing a hash of the query, and comparing the computed hash with the hash included in the information.

- Still another aspect of the invention from the point of view of the server is that the query package is constructed in a manner that a first part including at least the query is encrypted using a symmetric key of the user and a second part including at least the symmetric key of the user is encrypted using the public key of the provider, and the method further comprises decrypting the second part of the query package using the private key of the provider to obtain at

least the symmetric key of the user, and decrypting the first part of the query package using the symmetric key of the user to obtain at least the query.

- The present invention also comprises a stored message on a public bulletin board responsive to an anonymous query, **said message comprising a random number sequence and an associated encrypted electronic response package containing a response to the query, said response package being structured such that the response to the query can be obtained by the user by operations including a decryption with the private key of the user.**

- Another aspect of the inventive stored message is that the response package is constructed in a manner that a first part including at least the response is encrypted using a symmetric key of the provider and a second part including at least the symmetric key of the provider is encrypted using a public key of a user who made the anonymous query.

- Other objects, features and advantages of the present invention will become apparent upon perusal of the following detailed description when taken in conjunction with the appended drawing, wherein:

  In a first particular embodiment, the present invention includes a method for secure anonymous querying by **a user of a provider to whom a public key, private key pair is assigned, the public key of the provider being publicly obtainable by the user, the method comprising: formulating by the user of a query to be sent to the provider, generating by the user of a random number sequence, a public key of the user, and a**

corresponding private key of the user for sole use with said formulated query; forming an electronic encrypted query package by the user by operations including encryption with the public key of the provider obtained by the user, said electronic encrypted query package containing information including the formulated query, the generated random number sequence, the generated public key of the user, and an identification of a public bulletin board for posting a message comprising the random number sequence in association with an encrypted response to the query, and said query package being structured such that the contained information can be obtained by the provider **by operations including a decryption with the private key of the provider; and sending by the user of the query package to the provider via a network in a manner that the user is not identifiable to the provider, wherein the generated private key and the generated random number sequence are retained by the user.**

- In a first aspect of the first particular embodiment, the method further comprises: receiving by the provider via a network said query package sent by the user; obtaining by the provider by operations including decryption with the private key of the provider the information in said query package; formulating by the provider of a response to the query; **forming an electronic encrypted response package by the provider by operations include encryption with the public key of the user contained in said query package, said electronic encrypted response package containing the formulated response to the query**, said response package being structured such that the response to the query can be obtained by the user by operations including a decryption with the private key of the user; posting by the provider of a message comprising the random number sequence in association with the

response package to the identified public bulletin board; **accessing the identified bulletin board by the user in order to download the response package associated with that message posted by the provider including the random number sequence generated by the user; and obtaining by the user by operations including decryption with the private key of the user of the response information in said response package.**

Applicant notes the differences between the prior art cited and the pending application regarding the method of retrieval of the email. The method of the pending application does not disclose the use of a public key or PKI as a means to retrieve an email for an intended recipient from a public bulletin board.

4. THE METHOD OF POSTING A REPLY BY THE INTENDED RECIPIENT IN THE PENDING APPLICATION IS NOT DISCLOSED BY EPSTEIN

Applicant references the Epstein specification to further disclose:
The specific use of a private key <u>as the sole means by which a reply email is posted on a public bulletin board</u> is used to be retrieved by an intended recipient.

Applicant refers to column 2 line 1, through column 4 line 11 with the pertinent references highlighted.

- It is an object of the present invention to provide a method for queries in the form of electronic messages to be submitted securely and anonymously to an information provider via a public network, such as the Internet, and to provide a method for secure responses by the information provider which are obtainable by the inquiring party.

- Briefly, these and other objects are satisfied by a method, which from the point of view of the user, is for secure anonymous querying of a provider in which:

  a random number sequence, a public key of the user, and a corresponding private key of the user are generated;

  a public key of the provider is used to form an electronic encrypted query package containing information including a query, the generated random number sequence, and the generated public key of the user, the information including an identification of a public bulletin board for posting a message comprising the random number sequence in association with an encrypted response to the query, and the query package being structured such that the contained information can be obtained by the provider by operations including a decryption with the private key of the provider; and

  the query package is sent to the provider via a network in a manner that the user is not identifiable to the provider.

- Other aspects of the inventive method from the point of view of the user are that the query package is sent to the provider from a public terminal, and that a hash of the query is generated and is included in the information contained in the query package.

- A further aspect of the present invention is that a symmetric key of the user is generated and the query package is constructed in a manner that a first part including at least the query is encrypted using the generated symmetric key of the user and a second part

including at least the generated symmetric key of the user is encrypted using the public key of the provider.

- From the point of view of the information provider, the present invention is directed to a method for secure response by a provider to an anonymous query from a user in which:

an electronic encrypted query package containing information including a query, a random number sequence, and a public key of the user is received via a network, the information including an identification of a public bulletin board for posting a message comprising the random number sequence in association with an encrypted response to the query, and the query package being structured such that the contained information can be obtained by the provider by operations including a decryption with the private key of the provider;

the private key of the provider is used to obtain the information in said query package;

the public key of the user is used to form an electronic encrypted response package containing a response to the query, said **response package being structured such that the response to the query can be obtained by the user by operations including a decryption with the private key of the user; and**

a message comprising the random number sequence in association with the response package is posted to the identified public bulletin board.

- Another aspect of the present invention from the point of view of the server is that a hash of the query is included in the information contained in the query package, and the method further comprises computing a hash of the query, and comparing the computed hash with the hash included in the information.

- Still another aspect of the invention from the point of view of the server is that the query package is constructed in a manner that a first part including at least the query is encrypted using a symmetric key of the user and a second part including at least the symmetric key of the user is encrypted using the public key of the provider, and the method further comprises decrypting the second part of the query package using the private key of the provider to obtain at least the symmetric key of the user, and decrypting the first part of the query package using the symmetric key of the user to obtain at least the query.

- **The present invention also comprises a stored message on a public bulletin board responsive to an anonymous query, said message comprising a random number sequence and an associated encrypted electronic response package containing a response to the query, said response package being structured such that the response to the query can be obtained by the user by operations including a decryption with the private key of the user.**

- **Another aspect of the inventive stored message is that the response package is constructed in a manner that a first part including at least the response is encrypted using a symmetric key of the provider and a second part including at least the**

symmetric key of the provider is encrypted using a public key of a user who made the anonymous query.

- Other objects, features and advantages of the present invention will become apparent upon perusal of the following detailed description when taken in conjunction with the appended drawing, wherein:

In a first particular embodiment, the present invention includes a method for secure anonymous querying by a user of a provider to whom a public key, private key pair is assigned, the public key of the provider being publicly obtainable by the user, the method comprising: formulating by the user of a query to be sent to the provider, generating by the user of a random number sequence, a public key of the user, and a corresponding private key of the user for sole use with said formulated query; forming an electronic encrypted query package by the user by operations including encryption with the public key of the provider obtained by the user, said electronic encrypted query package containing information including the formulated query, the generated random number sequence, the generated public key of the user, and an identification of a public bulletin board for posting a message comprising the random number sequence in association with an encrypted response to the query, and said query package being structured such that the contained information can be obtained by the provider by operations including a decryption with the private key of the provider; and sending by the user of the query package to the provider via a network in a manner that the user is not identifiable to the provider, wherein the generated private key and the generated random number sequence are retained by the user.

- In a first aspect of the first particular embodiment, the method further comprises: receiving by the provider via a network said query package sent by the user; obtaining by the provider by operations including decryption with the private key of the provider the information in said query package; formulating by the provider of a response to the query; **forming an electronic encrypted response package by the provider by operations include encryption with the public key of the user contained in said query package, said electronic encrypted response package containing the formulated response to the query, said response package being structured such that the response to the query can be obtained by the user by operations including a decryption with the private key of the user; posting by the provider of a message comprising the random number sequence in association with the response package to the identified public bulletin board; accessing the identified bulletin board by the user in order to download the response package associated with that message posted by the provider including the random number sequence generated by the user; and obtaining by the user by operations including decryption with the private key of the user of the response information in said response package.**

Applicant notes the differences between the prior art cited and the pending application regarding the method of retrieval of the email. The method of the pending application does not disclose the use of a public key or PKI as a means to post a response email for an intended recipient to a public bulletin board.

U.S.C.§ 103 ANALYSIS

CLAIMS 46-48 AND 50-52 IN VIEW OF SYKES AND GABBER

In the Office Action, Examiner states[10]: that in reference to claims 46-48 and 50-52, Sykes discloses a method and system for archiving, registering, and verifying electronic communications transmitted between clients and recipients via a network (i.e. internet), (abstract and paragraph [0004], lines 1-13). Specifically, Examiner states that Sykes discloses the third party archiving and verification system to comprise: [11]

- The method for registering and certifying an electronic message, the system and method further comprising a client, an intended recipient, a website (i.e. third party archiving and verification website, Figures 4-22), a processing unit (i.e. third party archiving and verification server), an email database, a means (i.e. third party archiving and verification provider) to register the electronic message, the system and method, (abstract; paragraph [0004], lines 1-13; and paragraph [0038], line 1 to paragraph [0040], line 17), comprising the steps of:

---

[10] Application/Control Number 09/982,145, Office Action, pp 3-4.

[11] Application/Control Number 09/982,145, Office Action, pp 3-4.

- The client accessing the website and establishing a registration account; the processing unit assigning a code (i.e. account ID) to the registration account of the client, (paragraph [0048], line 1 to paragraph [0049], line 16 and Figure 4); and
- The processing unit receiving the electronic message, the electronic message being from the client; the processing unit storing information about the electronic message and the registration account in the email database; the **processing unit resending the electronic message to the intended recipient as identified by the client in the registration account**; the processing unit tracking the date the electronic message was sent by the processing unit; the processing unit tracking the date the electronic message was received by the intended recipient; the processing unit creating a confirmation record (i.e. message table entry) that comprises the date the electronic message was sent and the date the electronic message was received by the intended recipient; the processing unit sending the client a copy of the confirmation record (Figure 26); and the processing unit storing information about the confirmation record and the registration account in the email database, (paragraph [0038], line 1 to [0047], line 12; paragraph

[0059], line 1 to paragraph [0061], line 8; and paragraph [0065], lines 9-13).

Applicant argues that the above cited method Examiner states is disclosed in Sykes is not analogous to the method disclosed in the PENDING application, as amended in the second response to the Final Office Action. In fact, Applicant notes that the references to Sykes, as cited above, by the Examiner reads precisely as follows in the Sykes specification:

- A method and system for archiving and/or verifying electronic communications. The method and system provide verification of an email sent by a sender to a recipient, comprising receiving a copy of an email as an addressee; indexing the email according to at least one of sender, recipient, date, or subject matter**; and storing an exact copy of the email as received**. The method and system also provide for secure electronic communication between a sender and at least one recipient, comprising receiving from the sender view a secure internet connection a message and the email address of at least one intended recipient of the message; **sending an email message to the at least one intended recipient of the message that a message is waiting**; transmitting the message to the at least one intended recipient via a secure internet connection established by the at least one intended recipient; **and sending an email message to the sender that the at least one recipient has**

been sent the message. The method and system also provide for transmitting a facsimile for a sender to a recipient, the comprising: receiving an electronic facsimile message from the sender together with the facsimile number of the recipient; storing a copy of the electronic facsimile message; transmitting the facsimile message to the facsimile number of the recipient. [12]

- This invention relates to archiving and/or verifying electronic communications. According to a first aspect of the invention relating to sending verifiable email messages, the invention comprises addressing the email to a third party verification provider, either as an addressee or as a cc, who will index the message according to at least one of sender, date, recipient, and subject, and store an exact copy of the e-mail message. Similarly, the invention also relates to providing **email verification** of an email sent by a sender to a recipient, **comprising receiving a copy of an email as an addressee; indexing the email according to at least one of**

---

[12] Sykes abstract, US publication number 2002/0129108, as cited by Examiner in the Final Office Action, page 4, paragraph 3.

sender, recipient, date, or subject matter; and storing an exact copy of the email as received.[13]

- According to a first aspect, this invention relates to a **system and a method for senders to backup and archive email to a third party server without the need for conventional backup software, thereby providing proof of on-line communications**. The system and method are preferably implemented by a third party archiving and verification provider using an Application Service Provider ("ASP") model that allows a sender to use the system and method regardless of his or her location on the Internet. An example of the structure of tables in a SQL database for implementing the system and method of this invention is shown in Appendix A, attached hereto, and incorporated herein by reference. In the preferred embodiment, no special software is required, and an email sender can use the system without changing his standard email process.

Referring to FIG. 1, at 22 the sender sends an email to the recipient, and to the third party archiving and verification provider either as an addressee (via the "To:" field) or as a copy (via the

---

[13] Sykes specification, paragraph 004, US publication number 2002/0129108, as cited by Examiner in the Final Office Action, page 4, paragraph 3.

"CC:" field). Using any conventional email program, such as Outlook, Lotus Notes, Eudora, etc., the sender prepares an email to a recipient, and in the "To" field, or in the "CC:" field also addresses the email to the sender's account with the third party archiving and verification provider. For example an email sender would address the email, or copy the email, to his or her system account xxxxx@yyyyy.com, where xxxxx is a string identifying the sender's account with the third party archiving and verification provider, and where yyyyy.com is the third-party verification provider's email address.

At 24, the email message is received by the third party archiving and verification provider. At 26, a Message Transfer Agent (MTA), for example Sendmail, available from Sendmail, Emoryville, Calif., passes the email to a filter that generates an id based upon the time and date of receipt. The MTA is running on the system server. The email's id is preferably a 24 character identification code in the format yyyymmddhhmmssnnnnnnnnnn where yyyymmdd is an eight-character representation of the date of receipt, hhmmss is a six-character representation of the time of receipt, and nnnnnnnnnn is a unique ten-digit integer. At 28, the email message is written out to a queue directory based upon the id assigned to the email. At 30, a record is inserted into a queue table in the system's database,

which cues a cataloging daemon to begin processing the message. At 32 the MTA returns to processing incoming mail requests.[14]

- The third party verification provider's system includes at least one, and preferably more than one, cataloging daemons that monitor the queue table in the system database. The cataloging daemons also run on the system server. The number of cataloging daemons depends upon the CPU and the IO. Each cataloging daemon is assigned an id that corresponds to the queue table and the queue directories. The queue table has 2 fields: a queue number and a queue message ID. The queue directory is structured as: /gp/gpc1/outgoing, /gp/gpc1/incoming, /gp/gpc0/outgoing, and /gp/gpc0/incoming, and depending on the number of queues desired, the gpc(number) directory would be correspondingly increased. The same applies for an outgoing queue; a single process is in charge of it as well. When a cataloging daemon encounters an entry in its queue, it begins processing.

At 34, the header of the email message is read, based on RFC-822 internet mail standards, (which standards are incorporated herein by references as if fully set forth). At 36, each email address

---

[14] Sykes specification, US publication number 2002/0129108, paragraph 38, line 1, to paragraph 40, line 17.

in the "To:" and "CC:" lines of the email message's header are temporarily stored in an array, which may be a simple character pointer array. The "From:" line of the email message's header is temporarily stored separately. At 38, the cataloging daemon performs a lookup in an alias table of each email address to determine if that email address is a system account with the third party archiving and verification provider. If an email address is an account on the system, the cataloging daemon extracts the system's id for that account. At 40, if the address is valid, the email message's "Received:" header is verified with the MTA table. The MTA table is an extra security feature that stores and allows comparison with the mail relay authorized to deliver the email message to the account. This is an optional feature, that is preferably turned off by default for most accounts. The MTA table has 2 fields, user ID and the sender's MTA's host name. This ensures that the email message was sent from the proper internet mail relay, i.e. an email address that, according to the user's account profile, is authorized to send email to the account. At 42, if the internet mail relay is correct or if it is non-existent the cataloging daemon checks the email message's "From:" header against the address table to verify that the address is allowed to send to the system account. "Non-existent" means that no record is found in the MTA table for that user. This means that the user did not wish

to restrict email coming in based on their outgoing mail server. If the user does have an entry and that entry does not match the value in the MTA table, the message is rejected and an error email is placed in the queue for delivery to the user who sent the email. At 44, if the operations at 38, 40 and 42 are successful, the email message is passed to a catalogue routine, which is part of the cataloging daemon. If there is an error, appropriate error routines are called.

At 46, the email message's "To:", "From:", and "Subject:" lines and the message's size are stored in the system's message table, with the email message referred to by its assigned message id. The message table has the following fields: a) message id; b) user id; c) folder id (for later use in grouping messages); d) "To:" line; e) "From:" line; f) "Subject:" line; g) "Date:" line; h) "Time:" line; i) "Size:" line; j) expiration date; and k) has the message been paid for.

At 48, the archive matrix is used to determine the price of the email. The matrix, an example of which is shown in FIG. 3, is a cross of storage duration and message size. After the price of the email is determined, the price is inserted into the system's transaction table together with the email message's system id. The storage duration

is determined based upon the default value in the sender's account profile with the third party archiving and verification provider, unless the sender selects a different duration. At 50, a notification is written for each recipient in the email message to an outgoing message queue directory. The notification preferably includes the system message id, the date that the message was archived, and the original contents of the message including all attachments. A sample message is shown in FIG. 26. At 52 the cataloging daemon checks its particular queue and begins processing the next email message.

The email message remains stored with the third party archiving and verification provider for a time determined by the sender's user profile, which was established at the time the sender opened its account, as from time to time amended. Alternatively, the user could be allowed to select the time for storage at the time the message is sent. The user can also extend the time for storage later, as described below. **The third party verification provider preferably provides the sender with access to the stored email messages via a web browser, allowing the sender to manage the stored messages, deleting unneeded messages, extending the storage time for**

messages, and requesting verified copies of messages.[15] The system and method of the present invention provide a secure method for Internet users to communicate registered emails on the Internet without using conventional email clients such as Microsoft's Outlook Express or Netscape's Network Navigator. Instead, messages are created and read inside a web browser such as Microsoft's Internet Explorer, or Netscape's Navigator. Further, unlike conventional email, the system and method of this invention allow the sender to know if and when a message has been read. **The system and method allow the sender to see the state of any message, i.e., the user can see that the message has been delivered and read by the recipient, in contrast to conventional email where a user sends a message and is only notified when and if the recipient replies.** According to an alternate aspect of the invention, the system and method also allows the sender to receive an electronic or telephone reply to a needed request.

On the FIG. 7 "Main Menu--Welcome" page, the user would click "gProof Confidential" link, and reach the FIG. 20 page. From the

---

[15] Sykes specification, US publication number 2002/0129108, paragraph 41, line 1, to paragraph 47, line 12, as cited by Examiner in the Final Office Action, page 5, paragraph 1.

FIG. 20 page, the user the "Outbox" button to reach the FIG. 21 screen. On the FIG. 21 screen, the user is presented with an attachment box, an upload, and next buttons. As the user uploads files, they appear in the attachment box. Thee messages are stored on the system server as MIME entities. This preserves the content-type and other properties needed. The file names are defined as "internalMessageID.count++". After the user clicks the next button, the user is prompted with the "to", "from", "subject", and "body" form. The user is prompted with a confirmation of how much the message will cost and a "Send it" button.

As shown in FIG. 23, at 100, the Sender securely uploads email message to Third Party Archiving and Verification Provider. At 102, Third Party Archiving and Verification Provider emails Recipient that an message is waiting. At 104, Recipient securely downloads message from Third Party Archiving and Verification Provider. At 106, Third Party Archiving and Verification Provider emails Sender when Recipient receives message.[16]

---

[16] Sykes specification, US publication number 2002/0129108, paragraph 59, line 1, to paragraph 61, line 8.

- The user is able to check the status of the message and view the selection. A time and date stamp can be applied to show when the message was received, and when the selection was made.[17]

ANALYSIS OF SYKES SPECIFICATION, AS REFERENCED AND CITED BY THE EXAMINER IN THE OFFICE ACTION

Applicant respectfully submits that the above cited portions of the Sykes specification do not disclose the method of the PENDING application. Specifically, an analysis of the references to Sykes, as cited by the Examiner, fail to disclose the following novelties of the PENDING application.

1. THE METHOD OF DELIVERY OF THE EMAIL BY THE INDEPENDENT THIRD PARTY TO THE INTENDED RECIPIENT IN THE PENDING APPLICATION IS NOT DISCLOSED BY SYKES

Examiner states in her Office Action[18] that Sykes discloses: the system and method, (abstract; paragraph [0004], lines 1-13; and paragraph [0038], line 1 to paragraph [0040], line 17), comprising the steps of:

---

[17] Sykes specification, US publication number 2002/0129108, paragraph 65, line 9 to line 13, as cited by Examiner.

[18] Application/Control Number 09/982,145, Final Office Action, pp 4-5.

- The client accessing the website and establishing a registration account; the processing unit assigning a code (i.e. account ID) to the registration account of the client, (paragraph [0048], line 1 to paragraph [0049], line 16 and Figure 4); and
- The processing unit receiving the electronic message, the electronic message being from the client; the processing unit storing information about the electronic message and the registration account in the email database; the **processing unit resending the electronic message to the intended recipient as identified by the client in the registration account**; the processing unit tracking the date the electronic message was sent by the processing unit; the processing unit tracking the date the electronic message was received by the intended recipient; the processing unit creating a confirmation record (i.e. message table entry) that comprises the date the electronic message was sent and the date the electronic message was received by the intended recipient; the processing unit sending the client a copy of the confirmation record (Figure 26); and the processing unit storing information about the confirmation record and the registration account in the email database, (paragraph [0038], line 1 to [0047], line 12; paragraph

[0059], line 1 to paragraph [0061], line 8; and paragraph [0065], lines 9-13).

A review of the cited references to the Sykes specification, reveals that **Sykes fails disclose a method whereby the third party verification sends or resends the original message to the intended recipient**. Specifically, the portions of the Sykes specification, as cited by the Examiner in the Office Action, disclose the following method:

- A method and system for archiving and/or verifying electronic communications. The method and system provide verification of an email sent by a sender to a recipient, comprising receiving a copy of an email as an addressee; indexing the email according to at least one of sender, recipient, date, or subject matter; and storing an exact copy of the email as received. The method and system also provide for secure electronic communication between a sender and at least one recipient, comprising receiving from the sender view a secure internet connection a message and the email address of at least one intended recipient of the message; **sending an email message to the at least one intended recipient of the message that a message is waiting**; transmitting the message to the at least one intended recipient **via a secure internet connection established by the at least one intended recipient**; and sending an email message to the sender that the at least one

recipient has been sent the message. The method and system also provide for transmitting a facsimile for a sender to a recipient, the comprising: receiving an electronic facsimile message from the sender together with the facsimile number of the recipient; storing a copy of the electronic facsimile message; transmitting the facsimile message to the facsimile number of the recipient. [19]

Evidence that Sykes fails to disclose a delivery method as disclosed in the PENDING application is further found in the Sykes specification (and cited by the Examiner in her Office Action), whereby Sykes discloses:

- **As shown in FIG. 23, at 100, the Sender securely uploads email message to Third Party Archiving and Verification Provider. At 102, Third Party Archiving and Verification Provider emails Recipient that an message is waiting. At 104, Recipient securely downloads message from Third Party Archiving and Verification Provider**. At 106, Third Party Archiving and erification Provider emails Sender when Recipient receives message.[20]

---

[19] Sykes abstract, US publication number 2002/0129108, as cited by Examiner in the Final Office Action, page 4, paragraph 3.

[20] Sykes specification, US publication number 2002/0129108, paragraph 59, line 1, to paragraph 61, line 8, as cited by Examiner in the Final Office Action, page 5, paragraph 1.

In contrast, Applicant's method does not disclose a method of sending a "verifiable" email message by storing an exact copy of an email message received from a client, for future retrieval by an intended recipient, by way of a download from a website accessed by the intended recipient, per the method disclosed in Sykes.

Rather, the method disclosed in Applicant's application comprises a client sending a request for either a registered or certified email message to an independent third party provider (the "Processing Unit"). **The independent third party provider re-sends the email message directly to the intended recipient, as identified by the Client, from the Processing Unit.**

Specifically, Applicant refers to the specification of the PENDING application:

- The present inventive device is distinct from the prior art because it acts as an independent, verification that the e-mail was sent; said confirmation is achieved by the invention **sending the e-mail message on behalf of the sender**, tracking the electronic mail routing, and providing the client with a digital certificate that verifies the time and date when the electronic message was sent, and when it was received. [21]

---

[21] Nassiri specification, US Publication Number 2002/0046250, paragraph 21, line 1 to line 8.

- The present invention discloses a system, method and process to facilitate three primary functions as follow below.

  (i) Registered or Certified Email by an independent authority wherein the originator/sender of the electronic mail is identified. Method one is an independent verification that an electronic mail (including all attachments thereto) was sent to the intended recipient (as identified by the Client) and the time and date of submission (when the electronic mail was sent) and the time and date of delivery to the intended recipient. **Verification is a function of the processing unit who sends the electronic mail independent of the Client, albeit on behalf of the Client, who is identified as the sender/originator of the electronic message**. Upon delivery to the recipient, the Client shall receive a confirmation of the time and date in the form of a digital certificate.[22]

- Turning descriptively to the drawings, the Client utilizes the invention in one of three manners as disclosed above. With reference to FIG. 1, a Registered or Certified Email by an independent authority (the processing unit) is depicted wherein the originator/sender of the electronic mail is identified. In this embodiment, the Client (the sender/originator of the electronic mail)

---

[22] Nassiri specification, US Publication Number 2002/0046250, paragraph 45, line 1 to line 3; and paragraph 46, line 1 to line 14.

> sends the electronic mail to the intended recipient independently to the intended recipient. Additionally, the Client sends a copy of the email either independently, or as a "cc" or "bcc" to the Processing Unit. **The Processing Unit re-sends the email on the Client's behalf as a registered or certified electronic email message to the intended recipient, as identified by the Client.**[23]

Applicant submits that Sykes fails to disclose a method whereby a client has an independent third party provider send an original email message directly to an intended recipient and whereby the third party provider provides delivery confirmation in the form of a digital certificate. As such, Applicant submits that its method is not anticipated by Sykes and that claim 1 is patentable over Sykes.[24]

---

[23] Nassiri specification, US Publication Number 2002/0046250, paragraph 50, lines 1 to 13.

[24] Applicant notes that claim 29 of the PENDING application discloses a method whereby the intended recipient is advised via email that an email is "waiting" for the intended recipient at the Processing Unit. However, the method of delivery in claim 29 is analogous to that disclosed in the PENDING application; it is only temporary and is dependent on verification criteria input. That is, upon verification of the intended recipient's identity, the email is delivered directly to the intended recipient by the Processing Unit.

2. THE METHOD OF EMAIL "VERIFICATION" IN THE PENDING APPLICATION IS NOT DISCLOSED BY SYKES

In the Office Action, Examiner states[25] Sykes discloses a method and system for archiving, registering, and verifying electronic communications transmitted between clients and recipients via a network (i.e. internet), (abstract and paragraph [0004], lines 1-13). Specifically, Examiner states that Sykes discloses the third party archiving and verification system to comprise: [26]

- The method for registering and certifying an electronic message, the system and method further comprising a client, an intended recipient, a website (i.e. third party archiving and verification website, Figures 4-22), a processing unit (i.e. third party archiving and verification server), an email database, **a means (i.e. third party archiving and verification provider)** to register the electronic message, the system and method, (abstract; paragraph [0004], lines 1-13; and paragraph [0038], line 1 to paragraph [0040], line 17), comprising the steps of:
    - The client accessing the website and establishing a registration account; the processing unit assigning a code (i.e. account ID) to the registration account of the client,

---

[25] Application/Control Number 09/982,145, Office Action, pp 6-8.

[26] Application/Control Number 09/982,145, Office Action, pp 6-8.

(paragraph [0048], line 1 to paragraph [0049], line 16 and Figure 4); and

- The processing unit receiving the electronic message, the electronic message being from the client; the processing unit storing information about the electronic message and the registration account in the email database; the processing unit resending the electronic message to the intended recipient as identified by the client in the registration account; the processing unit tracking the date the electronic message was sent by the processing unit; the processing unit tracking the date the electronic message was received by the intended recipient; **the processing unit creating a confirmation record (i.e. message table entry) that comprises the date the electronic message was sent and the date the electronic message was received by the intended recipient; the processing unit sending the client a copy of the confirmation record (Figure 26)**; and the processing unit storing information about the confirmation record and the registration account in the email database, (paragraph [0038], line 1 to [0047], line 12; paragraph [0059], line 1 to paragraph [0061], line 8; and paragraph [0065], lines 9-13).

Applicant argues that the above cited "verification" method Examiner states is disclosed in Sykes is not analogous to the method disclosed in the PENDING application, as amended in the second response to the Final Office Action. In fact, Applicant notes that the references to Sykes, as cited by the Examiner, reads precisely as follow in the Sykes specification:

- A method and system for archiving and/or **verifying electronic communications.** The method and system provide verification of an email sent by a sender to a recipient, comprising receiving a copy of an email as an addressee; indexing the email according to at least one of sender, recipient, date, or subject matter**; and storing an exact copy of the email as received**. The method and system also provide for secure electronic communication between a sender and at least one recipient, comprising receiving from the sender view a secure internet connection a message and the email address of at least one intended recipient of the message; sending an email message to the at least one intended recipient of the message that a message is waiting; transmitting the message to the at least one intended recipient via a secure internet connection established by the at least one intended recipient; and sending an

email message to the sender that the at least one recipient has been sent the message. [27]

- This invention relates to archiving and/or verifying electronic communications. According to a first aspect of the invention relating to sending verifiable email messages, the invention comprises **addressing the email to a third party verification provider, either as an addressee or as a cc, who will index the message according to at least one of sender, date, recipient, and subject, and store an exact copy of the e-mail message**. Similarly, the invention also relates to providing **email verification** of an email sent by a sender to a recipient, **comprising receiving a copy of an email as an addressee; indexing the email according to at least one of sender, recipient, date, or subject matter; and storing an exact copy of the email as received.**[28]
- According to a first aspect, this invention relates to a **system and a method for senders to backup and archive email to a third party server without the need for conventional backup software, thereby providing proof of on-line communications**. The system and method are preferably implemented by a third

---

[27] Sykes abstract, US publication number 2002/0129108, as cited by Examiner.

[28] Sykes specification, US publication number 2002/0129108, as cited by Examiner.

party archiving and verification provider using an Application Service Provider ("ASP") model that allows a sender to use the system and method regardless of his or her location on the Internet. An example of the structure of tables in a SQL database for implementing the system and method of this invention is shown in Appendix A, attached hereto, and incorporated herein by reference. In the preferred embodiment, no special software is required, and an email sender can use the system without changing his standard email process.

- Referring to FIG. 1, at 22 the sender sends an email to the recipient, and to the third party archiving and verification provider either as an addressee (via the "To:" field) or as a copy (via the "CC:" field). ... At 24, the email message is received by the third party archiving and verification provider. ... **The email message remains stored with the third party archiving and verification provider for a time determined by the sender's user profile, which was established at the time the sender opened its account, as from time to time amended.** Alternatively, the user could be allowed to select the time for storage at the time the message is sent. The user can also extend the time for storage later, as described below.

Applicant argues that the method of verifying and/or confirming an email message in the PENDING application is not disclosed by Sykes. To state the

obvious, the present inventive device, offers archival only as an option for record keeping, and not as a mandatory means of verification of the email itself. As illustrated above, Sykes method of "verification" relies exclusively on archiving an exact copy of the original email for comparison at a future date, if needed. The internal (host computer of the verification and archive provider) verification record (i.e. the copy of the original email) is coupled with the time of submission and delivery of the original mandatory email. The original sender receives an email with the time and date that the email was received from the sender and when it was retrieved by the intended recipient.[29]

More importantly, and perhaps significantly, the method disclosed by Sykes does not verify the "contents" of an email, notwithstanding a "verification record", per the method disclosed in the PENDING application. To verify the content of an original email at a future date, the requesting (authorized) party must request a "notarized" version of the email from the archives of the verification provider as insurance against manipulation by an outside party[30]. In the method disclosed by Applicant's application, the contents of the original email message are contained in the verification record along with the time and date of submission and delivery of the email. **Depending on the service verification request, the confirmation record may also include biometric information, and other requested**

---

[30] Sykes specification, US publication number 2002/0129108, FIGS and 10 and 12.

information, such as a birth date or social security number. The contents of the verification record in its entirety are provided to the sender of the original email. The independent third party provider does not retain/archive a copy of the email contents, unless requested to by the original sender of the email. The only information archived by the independent third party provider is information regarding the time and date of submission and delivery and the code associated with the digital certificate that comprises the verification record. Specifically, the specification of the PENDING application discloses:

- The present invention discloses a system, method and process to facilitate three primary functions as follow below.
- Registered or Certified Email by an independent authority wherein the originator/sender of the electronic mail is identified. Method one is **an independent verification that an electronic mail (including all attachments thereto) was sent to the intended recipient (as identified by the Client) and the time and date of submission (when the electronic mail was sent) and the time and date of delivery to the intended recipient.** Verification is a function of the processing unit who sends the electronic mail independent of the Client, albeit on behalf of the Client, who is identified as the sender/originator of the electronic message. Upon delivery to the recipient, **the Client shall receive a confirmation of the time and date in the form of a digital certificate;**

- Registered or Certified Email by an independent authority wherein the originator/sender of the electronic mail is anonymous. **Method two is an independent verification that an electronic mail (including all attachments thereto) was sent to the intended recipient (as identified by the Client) and the time and date of submission (when the electronic mail was sent) and the time and date of delivery to the intended recipient.** Verification is a function of the processing unit who sends the electronic mail independent of the Client, albeit on behalf of the Client who is not identified. In this instance, the Processing Unit is identified as the sender of the electronic message only. Upon delivery to the recipient, **the Client shall receive a confirmation of the time and date in the form of a digital certificate**; and
- Registered or Certified Email by an independent authority wherein the originator/sender of the electronic mail requests that the recipient's identity be verified prior to receipt of the electronic mail. **Method three is an independent verification of the recipient's identity (as identified by the Client) by an independent authority prior to the recipient receiving the electronic mail. Per methods one and two above, in this instance, the independent authority (the processing unit) confirms the time and date of submission (when the electronic mail was sent) and the time and date of delivery to the intended recipient.**

Verification is a function of the processing unit who sends the electronic mail independent of the Client, albeit on behalf of the Client, who may or may not be identified. Upon delivery to the recipient, the **Client shall receive a confirmation of the time and date in the form of a digital certificate, and a confirmation that the intended recipient's identity was verified before receiving the electronic mail from the Client.**[31]

- The Processing Unit keeps an internal record of the account request and a copy of the email content (if requested). Upon personal identity verification, the Processing Unit submits the electronic message to the intended recipient, as identified by the Client in the registration account, and tracks the submission and delivery cycle of the electronic message. The electronic message indicates whether the Client is the originator of the email or whether the Processing Unit is sending the electronic message on behalf of an anonymous entity. **Upon delivery of the electronic message, the Processing Unit sends the Client a "Confirmation Record", typically in the form of a digital certificate, of the time and date of the submission and of the delivery of the electronic message. The Confirmation Record further contains the**

---

[31] Nassiri specification, US Publication Number 2002/0046250, paragraph 45, line 1 to paragraph 48, line 18.

information used to verify the intended recipient's identity.[32]

As noted above, not only are the verification records of the inventive devices different in substance, but in form. Sykes verification record to the sender of the original email comprises the form of an email with information contained within it. **The verification record of the present inventive device is in the form of a digital certificate that is tamper proof**; hence the distinction that the verification record disclosed by the PENDING application "verifies" the content of the email without the need to utilize the independent third party provider in the future .

Applicant submits that Sykes fails to disclose a method whereby the method of verification is based on information other than an archived record of the original email. As such, Applicant submits that its method is not anticipated by Sykes and is patentable over Sykes.

Applicant submits that Sykes fails to disclose a method whereby the third party provider provides a verification record in the form of a digital certificate. As such, Applicant submits that its method is not anticipated by Sykes and is patentable over Sykes.

Applicant submits that Sykes fails to disclose a method whereby the third party provider provides a verification record in the form of a digital certificate that

---

[32] Nassiri specification, US Publication Number 2002/0046250, paragraph 67, line 1 to line 18.

contains personal identity information. As such, Applicant submits that its method is not anticipated by Sykes and is patentable over Sykes.

Applicant submits that Sykes fails to disclose a method whereby the third party provider provides a verification record in the form of a digital certificate that contains biometric information. As such, Applicant submits that its method is not anticipated by Sykes is patentable over Sykes.

3. THE METHOD OF THE PROCESSING UNIT (INDEPENDENT THIRD PARTY VERIFICATION) IN THE PENDING APPLICATION IS NOT DISCLOSED BY SYKES

Applicant submits that the purpose and function of the independent third party verification provider in the PENDING application and that disclosed by Sykes are fundamentally distinct. In the PENDING application, the third party verification provider (in addition to being accessible via a website) comprises an actual physical place of business that can be accessed for the services disclosed in the specification: namely, a registered or certified email request, an anonymous registered or certified email request, or a request for identity verification of an intended recipient. With respect to the latter request, maintaining a physical presence is of the utmost importance in the event that the intended recipient be required to provide either original hard copy personal identity identification, or to provide biometrics as a proof of identity prior to receiving the intended email. Specifically, the method of the PENDING application discloses:

- **A request for identity verification prior to the receipt of registered or certified mail entails the Processing Unit contacting the intended recipient prior to sending the electronic message, and any attachments thereto**. The Processing Unit verifies that the email account to which the electronic message is to be routed corresponds to the identity of an intended recipient, prior to sending the electronic message. Alternatively, the Processing Unit may hold an electronic message on behalf of the sender, **whereby the intended recipient is verified in person at a service center maintained by the present invention**. Upon verification of the recipient's identity, the Processing Unit notifies the Client of when the electronic message was delivered to the intended recipient. Notification typically comprises a digital certificate that is emailed to the Client. If requested, the processing Unit retains a copy of the message contents, including any attachments, for future reference. In any event, the Processing Unit retains a record of the time and date the message was sent and when it was delivered for future reference.[33]
- Registered or Certified Email by an independent authority **wherein the originator/sender of the electronic mail requests that the recipient's identity be verified prior to receipt of the electronic mail. Method three is an independent verification of the recipient's identity (as identified by the Client) by an independent authority prior to the**

---

[33] Nassiri specification, US Publication Number 2002/0046250, paragraph 29, line 1 to line 20.

recipient receiving the electronic mail. Per methods one and two above, in this instance, the independent authority (the processing unit) confirms the time and date of submission (when the electronic mail was sent) and the time and date of delivery to the intended recipient. Verification is a function of the processing unit who sends the electronic mail independent of the Client, albeit on behalf of the Client, who may or may not be identified. Upon delivery to the recipient, the Client shall receive a confirmation of the time and date in the form of a digital certificate, and a confirmation that the intended recipient's identity was verified before receiving the electronic mail from the Client.[34]

- The Client selects the appropriate service by way of a pull down menu on the website with the available options: registered mail, certified mail, return receipt mail, delivery confirmation, submission confirmation, and the like, along with a request for Identity Verification. Identity shall be established by criteria selected by the sender using a pull down menu on the website. The recipient's identity may be verified by:

  (i) having the intended recipient using a predetermined electronic code provided by the Client; or

  (ii) having the intended recipient using a predetermined electronic code provided by the Processing Unit;

  (iii) having the intended recipient go to a Processing Unit service center for

---

[34] Nassiri specification, US Publication Number 2002/0046250, paragraph 48, line 1 to line 18.

an in-person verification using the intended recipient's personal identification, including, but not limited to, personal paperwork such as a birth certificate, a passport, a driver's license and the like; or

(iv) having the intended recipient provide bio-metric verification; or

(v) other means whereby the intended recipient utilizes a predetermined code, a password or other means of encryption.[35]

- "Identity Verification" denotes a variety of services offered by the inventive device. The services may comprise, but are not limited to, verification using digital certificates, biometric information such as a thumbprint, voiceprint, retinal scan, a graphical, hand written signature, or personal identity papers such as a drivers license, a passport, and the like.[36]

In contrast, the method disclosed by Sykes fails to disclose any method of identity verification prior to an intended recipient being allowed to access its website to download the waiting email. The method of Sykes fails to disclose the ability of the sender to independently request that the recipient be identified by either personal identity documents or biometric information. In fact, the method disclosed by Sykes is incapable of providing any identification verification services as a priori to receiving the email. In fact, the method disclosed by Sykes

---

[35] Nassiri specification, US Publication Number 2002/0046250, paragraph 58, line 1, to paragraph 63, line 3.

[36] Nassiri specification, US Publication Number 2002/0046250, paragraph 84, line 1 to line 7.

only verifies that the intended recipient's email address is registered in order to gain access to the website to download the email being held for the intended recipient. Specifically, the method of Sykes discloses:

- Where the recipient does not have an account with the Third Party Archiving and Verification Provider, the system and method can include a verification system to make sure that the message is delivered to the proper recipient. As described above, when the sender clicks the "Confirm" button on the FIG. 21 page, the system checks to see if the addressee in the "To:" has an account with the Third Party Archiving and Verification Provider. If the recipient does not have an account, the system sends an email that instructs the user to go to Third Party Archiving and Verification Provider's website and create an account. After the recipient creates an account, with the Third Party Archiving and Verification Provider's website, the system generates a 64 character string that relates to that user's email address. The system then sends an email to that address with the 64 character ID embedded in a link. When recipient clicks on that link, the system verifies that the recipient's email address is valid because they referenced an ID that was sent to that email address. The same ID is mapped to the same address in the Third Party Archiving and Verification Provider's database. After the user clicks the link, the Third Party Archiving and Verification Provider's system marks the recipient's account as active, then searches the database for any email messages that do not yet have an ID assigned to it, and which also have

the recipient's email address in the "To:" line. After the system finds the email messages meeting these criteria, the messages are then assigned to that userID. Thus when the recipient logs in for the first time, the message or messages addressed to the recipient will be waiting for the recipient.[37]

Moreover, there exist fundamental issues between the method disclosed in Sykes and the present inventive device with respect to access to the archived records and management of the archived records. The method disclosed in the PENDING application does not permit retrieval of archival records by outside parties, or manipulation of archived records by outside parties. Management and control of the verification records is controlled by the independent third party provider, and access (i.e. requesting a copy of the archived confirmation record) is restricted to the original client that tendered the service request, or an authorized third party, as designated by the independent third party provider. In contrast, the method disclosed by Sykes allows the originator of the email to access the archived files, and to manipulate the archived files according to the needs of the account holder. Specifically, Sykes discloses a method whereby:

- **The third party verification provider preferably provides the sender with access to the stored email messages via a web browser, allowing the sender to manage the stored messages, deleting**

---

[37] Sykes specification, US publication number 2002/0129108, paragraph 63, line 1 to line 30.

unneeded messages, extending the storage time for messages, and requesting verified copies of messages.[38]

- The system and method of the present invention provide a secure method for Internet users to communicate registered emails on the Internet without using conventional email clients such as Microsoft's Outlook Express or Netscape's Network Navigator. Instead, messages are created and read inside a web browser such as Microsoft's Internet Explorer, or Netscape's Navigator. Further, unlike conventional email, the system and method of this invention allow the sender to know if and when a message has been read. **The system and method allow the sender to see the state of any message, i.e., the user can see that the message has been delivered and read by the recipient, in contrast to conventional email where a user sends a message and is only notified when and if the recipient replies.**[39]

Applicant submits that Sykes fails to disclose a method whereby the independent third party provider provides a verification of identity as a priori to the intended

---

[38] Sykes specification, US publication number 2002/0129108, paragraph 47, line 8, to line 12.

[39] Sykes specification, US publication number 2002/0129108, paragraph 59, line 1 to line 14.

recipient receiving the email. As such, Applicant submits that its method is not anticipated by Sykes and that claim 1 is patentable over Sykes.

Applicant submits that Sykes fails to disclose a method whereby the independent third party provider maintains exclusive control and dominion over the archived confirmation records. As such, Applicant submits that its method is not anticipated by Sykes is patentable over Sykes.

CONCLUSION IN VIEW OF SYKES

Applicant submits that Sykes fails to disclose a method whereby a client has an independent third party provider send an original email message directly to an intended recipient and whereby the third party provider provides delivery confirmation in the form of a digital certificate. As such, Applicant submits that its method is not anticipated by Sykes and is patentable over Sykes.

Applicant submits that Sykes fails to disclose a method whereby the method of verification is based on information other than an archived record of the original email. As such, Applicant submits that its method is not anticipated by Sykes and is patentable over Sykes.

Applicant submits that Sykes fails to disclose a method whereby the third party provider provides a verification record in the form of a digital certificate. As such, Applicant submits that its method is not anticipated by Sykes and is patentable over Sykes.

Applicant submits that Sykes fails to disclose a method whereby the third party provider provides a verification record in the form of a digital certificate that contains personal identity information. As such, Applicant submits that its method is not anticipated by Sykes and is patentable over Sykes.

Applicant submits that Sykes fails to disclose a method whereby the third party provider provides a verification record in the form of a digital certificate that contains biometric information. As such, Applicant submits that its method is not anticipated by Sykes and is patentable over Sykes.

Applicant submits that Sykes fails to disclose a method whereby the independent third party provider provides a verification of identity as a priori to the intended recipient receiving the email. As such, Applicant submits that its method is not anticipated by Sykes and is patentable over Sykes.

Applicant submits that Sykes fails to disclose a method whereby the independent third party provider maintains exclusive control and dominion over the archived confirmation records. As such, Applicant submits that its method is not anticipated by Sykes and is patentable over Sykes.

Applicant respectfully submits that Examiner withdraw its objections and that Applicant's claims 46-48 and 50-52 be allowed per the arguments put forth above.

Applicant notes that Examiner states:

Although Sykes discloses substantial features of the claimed invention, the reference fails to explicitly disclose the method comprising; an anonymous client, a local computing system, the anonymous client using the local computing system to access a website; the processing unit notifying the intended recipient that the electronic message has been sent on behalf of the anonymous client; the intended recipient choosing to post a reply for the anonymous client, and the confirmation record comprising the reply posted for the anonymous client. Nonetheless, these features would have been obvious modifications to the aforementioned method, as disclosed by Sykes, for one of ordinary skill in the art at the time of the invention, as further evidenced by Gabber.[40]

Applicant submits that Sykes clearly fails to disclose the use of an anonymous client, as pointed out by the Examiner. Applicant respectfully submits that the disclosure of the present inventive device is not an obvious modification to the method disclosed in the pending application. Examiners must consider comparative data in the specification which is intended to illustrate the claimed invention in reaching a conclusion with regard to the obviousness of the claims.[41] Too, When obviousness is based on the teachings of multiple prior art

---

[40] Application/Control No. 09/982,145, Final Office Action, page 8, paragraph 2.

[41] *In re Margolis*, 785 F.2d 1029, 228 USPQ 940 (Fed. Cir. 1986).

references, the movant must also establish some "suggestion, teaching, or motivation" that would have led a person of ordinary skill in the art to combine the relevant prior art teachings in the manner claimed.[42] This is because "[c]ombining prior art references without evidence of such a suggestion, teaching, or motivation simply takes the inventor's disclosure as a blueprint for piecing together the prior art to defeat patentability—the essence of hindsight." Dembiczak, 175 F.3d at 999. Therefore, we have consistently held that a person of ordinary skill in the art must not only have had some motivation to combine the prior art teachings, but some motivation to combine the prior art teachings in the particular manner claimed.[43]

The failure of others to provide a feasible solution to a longstanding problem is probative of non-obviousness. The "rationale here is that if the patented solution were obvious, others would have come up with the solution first."[44] Applicant notes that in the method disclosed by Sykes, despite the detailed disclosure of the options available to the end user (the sender), **there exists no mention of the use of an alias or an anonymous identity to shield the original sender.**[45] Applicant further submits, that despite the detailed disclosure of Sykes, **there**

---

[42] See *Tec Air, Inc. v. Denso Mfg. Mich. Inc.*, 192 F.3d 1353, 1359-60 (Fed. Cir. 1999); *Pro-Mold & Tool Co. v. Great Lakes Plastics, Inc.*, 75 F.3d 1568, 1572 (Fed. Cir. 1996).

[43] See, e.g., *In re Kotzab*, 217 F.3d 1365, 1371 (Fed. Cir. 2000).

[44] *Indian Head*, 859 F Supp at 1104, 36 USPO 2d at 1323.

[45] Sykes specification, US Publication No. 2002/0129108, FIGS 1 to 27.

exists no mention of a third party provider that clearly indicates the third party provider is acting on behalf of the anonymous original sender, per the method disclosed in the pending application.

CONCLUSION IN VIEW OF SYKES

Applicant submits that Sykes fails to disclose a method whereby an anonymous client may send either a registered or a certified email message using a third party provider. As such, Applicant submits that its method is not anticipated by Sykes is patentable over Sykes.

Applicant submits that Sykes fails to disclose a method whereby the third party provider notifies the intended recipient that the electronic message has been sent on behalf of the anonymous client, and whereby the third party provider identifies itself as the sender. As such, Applicant submits that its method is not anticipated by Sykes and is patentable over Sykes.

Applicant submits that Sykes fails to disclose a method whereby the intended recipient may choose to post a reply email message for the anonymous client, using the third party provider as an intermediary. As such, Applicant submits that its method is not anticipated by Sykes is patentable over Sykes.

Applicant submits that Sykes fails to disclose a method whereby the confirmation record comprises the reply email message posted for the anonymous client from the intended recipient, and whereby said confirmation record is sent to the

anonymous client. As such, Applicant submits that its method is not anticipated by Sykes and is patentable over Sykes.

With regard to Sykes, Applicant respectfully submits that Examiner withdraw its objection and that Applicant's claims be allowed per the arguments put forth above.

CLAIMS 46-48 AND 50-52 IN VIEW OF GABBER

Examiner states that:

> In an analogous art, Gabber discloses a method for transmitting electronic messages between an anonymous client and a recipient via a computer network (i.e. Internet), (abstract and column 2, line 52 to column 3, line 2). Gabber further discloses the method involves employing a local computing system (Figure 1-item 105a), and the client using the local computing system to access a website (column 4, line 20 to column 5, line 7). Gabber also discloses a processing unit (i.e. Figure 2), (column 5,line 25-36), notifying (i.e. substituted real source address with alias address consisting of a printable string of characters) the intended recipient that the electronic message has been sent on behalf of the anonymous client, (column 6, line 41 to column 7, line 6); and the intended recipient choosing to post a reply for the anonymous client, (column 8, lines 27-50), These modifications to

> the aforementioned method, as disclosed by Sykes, would have been obvious to one of ordinary skill in the art because one would have been so motivated to facilitate "bi-directional e-mail communication over a network without compromising the sender's identity", and thereby increasing user privacy, (Gabber column 2, lines 1-5).[46]

Applicant respectfully traverses. Applicant submits that Gabber fails to disclose the method of the pending application, as disclosed in the specification and the amended claims. Applicant is mindful of Examiner's second objection that "the features upon which Applicant relies (i.e. that the client remain anonymous but the email address that sends the email message to the intended recipient remains constant and verifiable) are not recited in the rejected claims."[47] Applicant has amended the claim language to address the Examiner's concerns and submits further remarks with respect to Gabber.

Applicant refers to the Gabber specification, as cited by the Examiner, which reads:

- A system for, and method of, **generating an alias source address** for an electronic mail ("e-mail") message having a real source address and a

---

[46] Application/Control No. 09/982,145, Final Office Action, page 8, paragraph 3, to page 9, paragraph 1.

[47] Application/Control No. 09/982,145, Final Office Action, page 3, paragraph 2.

destination address and a computer network, such as the Internet, including the system or the method. In one embodiment, the system includes an alias source address generator that employs the destination address to generate the alias source address. **The system further includes an alias source address substitutor that substitutes the alias source address for the real source address. This removes the real source address from the e-mail message and thereby renders the sender, located at the real source address, anonymous.** Further-described are systems and methods for forwarding reply e-mail and filtering reply e-mail based on alias source address.[48]

- To address the above-discussed deficiencies of the prior art, the present invention introduces a system for and method of, generating an alias source address for an electronic mail ("e-mail") message having a real source address and a destination address and a computer network, such as the Internet, including the system or the method. In one embodiment, the system includes an alias source address generator that employs the destination address to generate the alias source address. The system further includes an alias source address substitutor that substitutes the alias source address for the real source address. **This removes the real source address from the e-mail message and thereby renders the sender, located at the real source address, anonymous.** The system further includes an e-mail forwarder that receives e-mail addressed to the

---

[48] Gabber abstract, United States Patent No. 6,591,291.

alias source address, computes the real source address, and forwards the e-mail to the real source address.[49]

- The method 300 ends in an end step 370, derivation of the alias source address having been accomplished. As with all of the other steps 310, 320, 330, 340, 350, the step 360 is unnecessary, unless the desired result is an alias source address consisting of a printable string of characters. The alias source address may then be substituted for the real source address, perhaps with an alias source address substitutor. Employing the above-described exemplary method 300 to an e-mail message having a real source address of, for example, "foo_bar@bell-labs.com" and a destination address of "www.yahoo.com" can be converted to "wxOnlqlUUEXJxzwVSsfKgW". This can be pre-appended to the domain name and top-level domain of an exemplary remailer to yield: "wxOnlqlUUEXJxzwVSsfKgW@lpwa.com", a destination-address-specific, SMTP-valid, alias source address. Employing a less complex method wherein the compressing, hashing, appending and encrypting, as set forth in the method 300 above, do not occur can yield different results. For example, an e-mail message having a real source address of, for example, "foo_bar@bell-labs.com" and a destination address of "www.yahoo.com" can be converted to "foo_bar.bell-labs.com.www.yahoo.com" (nothing more than a trivial string

---

[49] Gabber Summary of Invention, United States Patent No. 6,591,291, column 2, line 52, to column 3, line 2.

concatenation). This can be pre-appended to the domain name and top-level domain of an exemplary remailer to yield: "www.yahoo.com.foo_bar.bell-labs.com@lpwa.com". This far less complex (and less secure) method falls well within the broad scope of the present invention, as well. Note that the steps set forth in the method 300 are not employed in the less complex method.[50]

- Accordingly, the method 400 begins in a start step 410 and proceeds to a step 420, wherein a reply e-mail message is received from the recipient. **The method 400 continues in a step 430, wherein the alias source address is read from the reply e-mail message. Next, the alias source address is compared to alias source addresses contained in a sender-supplied list of rejected alias source addresses in a decisional step 440. If the alias source address matches one of the items in the list (taking the YES branch of the decisional step 440, the reply e-mail is deleted and the sender spared of its receipt.** If the alias source address does not match any of the items in the list (taking the NO branch of the decisional step 440, the method continues in a step 450 wherein the sender's real source address is derived (perhaps by reversing the exemplary method 300 described above or perhaps by way of a real source address generator that generates a real source address from an alias source address) and substituted into the reply e-mail for the alias

---

[50] Gabber, United States Patent No. 6,591,291, column 6, line 41, to column 7, line 6.

source address, perhaps by way of a real source address substitutor. Next, the reply-e-mail is forwarded to the sender in a step 460. The method ends in an end step 470, filtered forwarding having been accomplished.[51]

With respect to the foregoing references cited by the Examiner in the final Office Action Applicant submits that Gabber fails to disclose the method of the pending application.

Applicant submits that in its entirety Gabber fundamentally discloses a method that comprises sending an **"alias source email message"**, the purpose of which is to generate emails that are untraceable, as is typical in the case of spam or phishing. Gabber does not disclose a method, per the present inventive device, whereby the sender of the email can be readily ascertained and replied to. In fact, Gabber specifically states that one the inventive devices attributes is; " privacy (the recipient can not determine the real source address given the alias source address".[52]

---

[51] Gabber, United States Patent No. 6,591,291, column 8, line 27 to line 50

[52] Gabber, United States Patent No. 6,591,291, column 3, line 40 to line 43.

The "anonymous client"[53] Examiner attributes per the method of Gabber is distinct from the "anonymous client" as disclosed in the pending application. Moreover, Applicant respectfully submits that the Gabber specification **at no point refers to an "anonymous client" and that the reference is not analogous in method or definition to the disclosure of the PENDING application.**

Specifically, the Gabber specification consistently refers to an "alias source email address".[54] Said alias email address having the function of replacing a verifiable email address for the purpose of deceiving the intended recipient of the origin of the email message.

Per the Examiner's cited reference, Gabber specifically discloses a method whereby:

- [the] substitutor that substitutes the alias source address for the real source address. This removes the real source address from the e-mail message. **This removes the real source address from the e-mail**

---

[53] Application/Control No. 09/982,145, Final Office Action, page 8, paragraph 3.

[54] For this reason, Applicant prefers to refer to Gabber as an "alias source email address". Applicant respectfully submits that no text or disclosure in Gabber's specification supports the contention of an "anonymous client" per the method of claim 15 in the pending application. Rather, an anonymous email address.

message and thereby renders the sender, located at the real source address, anonymous.[55]

The method of Gabber discloses **generating an alias source email address for an electronic mail message** having a real source address and a destination address. While providing the client with an alias source email address indirectly serves to shroud the client's identity, per the method disclosed by Gabber, **there is no correlation between the alias source email address generated and the sender to identify the sender of the email message.**

In contrast, the method disclosed in the pending application clearly identifies the sender of the email. Specifically, the pending application discloses:

- Registered or Certified Email by an independent authority wherein the originator/sender of the electronic mail is anonymous. Method two is an independent verification that an electronic mail (including all attachments thereto) was sent to the intended recipient (as identified by the Client) and the time and date of submission (when the electronic mail was sent) and the time and date of delivery to the intended recipient. **Verification is a function of the processing unit who sends the electronic mail independent of the Client, albeit on behalf of the Client who is not**

---

[55] Gabber, United States Patent No. 6,591,291, column 2, line 52, to column 3, line 2.

identified. In this instance, the Processing Unit is clearly identified as the sender of the electronic message.[56]

- The Processing Unit keeps an internal record of the account request and a copy of the email content (if requested). The Processing Unit submits the electronic message to the intended recipient, as identified by the Client in the registration account, and tracks the submission and delivery cycle of the electronic message. **In this embodiment of the present invention, The Client remains anonymous and the Processing Unit is identified as the sender of the email. The recipient is notified by the Processing Unit that the Processing Unit is acting as a delivery vehicle for an anonymous identity, and that the originator of the message will be notified of the delivery to the recipient. Should the recipient elect, recipient has the option of posting a reply for the originator of the electronic message with the Processing Unit.** Upon delivery of the anonymous electronic message, the Processing Unit sends the Client a "Confirmation Record", typically in the form of a digital certificate, of the time and date of the submission and of the delivery of the electronic message.[57]

---

[56] Nassiri specification, US Publication Number 2002/0046250, paragraph 0047, line 1 to line 12.

[57] Nassiri specification, US Publication Number 2002/0046250, paragraph 56, line 1 to line 22.

Applicant's claim 15 clearly discloses a method whereby while the client remains anonymous, **the email address that sends the email message to the intended recipient is a disclosed identity that remains constant and verifiable** (i.e., not an alias source email address whereby the intended recipient has no way of deciphering the source, per the method of Gabber[58]). Per the method disclosed in Applicant's claim 15, the identity of the email address sender (the third party provider) is readily provided, **only the identity of the client utilizing the third party provider is withheld from the intended recipient.**

Examiner further cites that Gabber discloses notifying (i.e. substituted real source address with alias address consisting of a printable string of characters) the intended recipient that the electronic message has been sent on behalf of the anonymous client[59], and that the intended recipient may choose to post a reply for the anonymous client. With respect to Examiner's position that Gabber discloses notifying the intended recipient that an electronic message has been sent on behalf of the anonymous client, Applicant respectfully submits that the Gabber specification fails to disclose such a method.

---

[58] Gabber discloses a process whereby the address created bears no correlation to the sender of the sender, other than a formulaic computation. Gabber, United States Patent No. 6,591,291, column 6, line 41, to column 7, line 6.

[59] Application/control No. 09/982,145, Final Office Action, page 8, paragraph 3.

The prior art cited by the Examiner specifically reads as follows:

- The method 300 ends in an end step 370, derivation of the alias source address having been accomplished. As with all of the other steps 310, 320, 330, 340, 350, the step 360 is unnecessary, unless the desired result is an alias source address consisting of a printable string of characters. The alias source address may then be substituted for the real source address, perhaps with an alias source address substitutor. Employing the above-described exemplary method 300 to an e-mail message having a real source address of, for example, "foo_bar@bell-labs.com" and a destination address of "www.yahoo.com" can be converted to "wxOnlqlUUEXJxzwVSsfKgW". This can be pre-appended to the domain name and top-level domain of an exemplary remailer to yield: "wxOnlqlUUEXJxzwVSsfKgW@lpwa.com", a destination-address-specific, SMTP-valid, alias source address. Employing a less complex method wherein the compressing, hashing, appending and encrypting, as set forth in the method 300 above, do not occur can yield different results. For example, an e-mail message having a real source address of, for example, "foo_bar@bell-labs.com" and a destination address of "www.yahoo.com" can be converted to "foo_bar.bell-labs.com.www.yahoo.com"

(nothing more than a trivial string concatenation). This can be pre-appended to the domain name and top-level domain of an exemplary remailer to yield: "www.yahoo.com.foo_bar.bell-labs.com@lpwa.com". This far less complex (and less secure) method falls well within the broad scope of the present invention, as well. Note that the steps set forth in the method 300 are not employed in the less complex method.[60]

The foregoing method disclosed by Gabber does not "notify" the intended recipient that said intended recipient has received a message on behalf of an anonymous client. It may be self-evident to the intended recipient that the source email address has been morphed to conceal the identity of the sender, per the method of Gabber, but the **foregoing method does not constitute notification as disclosed in the method of Applicant's claim 15, whereby the intended recipient receives an email message from the third party provider, clearly disclosing that the third party provider is sending an email message on behalf of an anonymous client.**[61]

---

[60] Gabber, United States Patent No. 6,591,291, column 6, line 41 to column 7, line 6.

[61] Nassiri specification, US Publication Number 2002/0046250, paragraphs 47 and 56.

Likewise, Examiner submits that Gabber discloses a method whereby the intended recipient may choose to post a reply for the anonymous client.[62] Applicant submits that while the recipient may respond to an alias source email message by hitting the reply button, the response email message must first pass a check sum to qualify the response, before the email message response will be received. **Moreover, the intended recipient is remains unable to decipher to whom the response is directed, other than to an alias source email address**. The originator of the email message to whom the response is directed remains a secret or unidentifiable.

The method disclosed in Applicant's claim 15 clearly identifies to whom the response is directed to, the verifiable independent third party provider, and requires no qualification that the response email message from the intended recipient satisfy a check sum test in order to be received.

CONCLUSION IN VIEW OF GABBER

Applicant submits that Gabber fails to disclose a method that comprises an anonymous client as disclosed in the pending application. As such, Applicant submits that its method is not anticipated by Gabber and is patentable over Gabber.

---

[62] Gabber, United States Patent No. 6,591,291, column 8, line 27 to line 50.

Applicant submits that Gabber fails to disclose a method whereby an anonymous client may send either a registered or a certified email message using a third party provider. As such, Applicant submits that its method is not anticipated by Gabber and is patentable over Gabber.

Applicant submits that Gabber fails to disclose a method whereby an anonymous client may send either a registered or a certified email message using a third party provider. As such, Applicant submits that its method is not anticipated by Gabber and is patentable over Gabber.

Applicant submits that Gabber fails to disclose a method whereby the third party provider tracks the date the email message was sent, and the date that the email message was received by the intended recipient. As such, Applicant submits that its method is not anticipated by Gabber and is patentable over Gabber.

Applicant submits that Gabber fails to disclose a method whereby the third party provider creates a confirmation record that comprises the date sent data and the date received data. As such, Applicant submits that its method is not anticipated by Gabber and is patentable over Gabber.

Applicant submits that Gabber fails to disclose a method whereby the anonymous client receives a copy of the confirmation record from the third party provider. As such, Applicant submits that its method is not anticipated by Gabber and is patentable over Gabber.

Applicant submits that Gabber fails to disclose a method whereby the confirmation record is archived for future use and retrieval. As such, Applicant submits that its method is not anticipated by Gabber and is patentable over Gabber.

Applicant submits that Gabber fails to disclose a method whereby the third party provider notifies the intended recipient that the email message has been sent on behalf of the anonymous client by the third party provider. As such, Applicant submits that its method is not anticipated by Gabber and is patentable over Gabber.

Applicant submits that Gabber fails to disclose a method whereby the third party provider clearly identifies itself as the sender of the email message, with a verifiable, constant email address, along with other identifying information. As such, Applicant submits that its method is not anticipated by Gabber and is patentable over Gabber.

Applicant submits that Gabber fails to disclose a method whereby the intended recipient may choose to post a reply email message for the anonymous client, using the third party provider as an intermediary, and whereby the response email message need not satisfy a check sum test. As such, Applicant submits that its method is not anticipated by Gabber and is patentable over Gabber.

Applicant submits that Gabber fails to disclose a method whereby the confirmation record comprises the reply email message posted for the

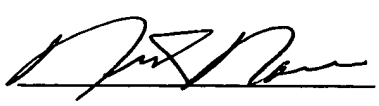
anonymous client from the intended recipient, and whereby said confirmation record is sent to the anonymous client. As such, Applicant submits that its method is not anticipated by Gabber and is patentable over Gabber.

With regard to Gabber, Applicant respectfully submits that Examiner withdraw its objection and that Applicant's claims be allowed per the arguments put forth above.

CLAIMS 46-48 AND 50-52 IN VIEW OF SYKES, BYRD AND EPSTEIN

Applicant submits that the stated grounds of rejection in the pending claims have been properly traversed, accommodated, or rendered moot. Applicant therefore respectfully requests that the Examiner reconsider and withdraw the presently outstanding rejections. It is believed that a full and complete response has been made to the outstanding Office action, and as such, the present application is in condition for allowance. Thus, prompt and favorable consideration of this amendment is respectfully requested.

Respectfully Submitted,



Nick Nassiri